


	EUMETSAT POLAR SYSTEM	<i>EUMETSAT</i> 
		Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97

DATA DENIAL **IMPLEMENTATION ON METOP**

Technical Note



	EUMETSAT POLAR SYSTEM	EUMETSAT 
		Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97

DOCUMENT SIGNATURE TABLE

	Name	Function	Signature	Date
Author	A. Boissin	System Engineer		
Approval				
Approval	B. Marcorelles	System Manager		
Release	M. Langevin	Programme Manager		

© , EUMETSAT

The Copyright of this document is the property of EUMETSAT. It is supplied in confidence and shall not be reproduced, copied or communicated to any third party without written permission from EUMETSAT.

	EUMETSAT POLAR SYSTEM	EUMETSAT 
		Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97

DISTRIBUTION LIST

Internal Distribution	
Name	No. Copies
LEO/ML	1
LEO/PAB	1
LEO/AIB	1
LEO/JP	1
GSD/Hhu	1
COL/SGC	1
GSD/RW	1
GSD/JG	
OPS/RH	

External Distribution		
Company	Name	No. Copies
NOAA	NPOES Programme Manager	1





	EUMETSAT POLAR SYSTEM	EUMETSAT 
		Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97

TABLE OF CONTENTS

1	INTRODUCTION	2
1.1	Purpose and Scope	2
1.2	Reference Document	2
1.3	Data denial objectives	2
1.4	Structure of the document	3
2	ENCRYPTION SYSTEM TECHNICAL DESCRIPTION	4
2.1	General background	4
2.2	EPS / METOP Encryption concept	6
2.2.1	DES Keys definition	6
2.2.2	Encryption / decryption principle	8
2.2.3	Stations decryption concept	11
2.3	Keys Management concept	12
2.3.1	Users station registration and data access management	12
2.3.2	On board encryption configuration	13
2.3.3	Encryption scheduling; MGK generation	15
3	DATA DENIAL: OPERATIONAL PROCEDURES	16
3.1	3.1 Director's list	16
3.2	3.2 Sequence of actions	17
3.3	3.3 Instrument's list	18
3.4	Additional Security features	19
3.4.1	Master Keys	19
3.4.2	Authentication of Users Stations Public Keys	19
3.4.3	Key Management Center protection	19
3.4.4	Users Stations Master and Public Keys distribution	19

	EUMETSAT POLAR SYSTEM	EUMETSAT 
		Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97

2 INTRODUCTION

2.1 Purpose and Scope

This document describes the implementation of the Data Denial requirements expressed in NOAA Cooperation Agreement within the EPS/METOP System. Because this implementation is an operational implementation of the EPS encryption system specification, the principle governing the EPS Encryption specification are recalled in chapter 2.

2.2 Reference Document

- RD 1: Cooperation Agreement between NOAA and EUMETSAT
- RD2: EPS Encryption System Specification
EPS/SYS/SPE/95424
- RD3: EPS / METOP System Requirement Document
EPS/SYS/REQ/93001
- RD4: ESA / EUMETSAT: "HRPT / LRPT Direct Broadcast Services Specification"
MO-DS-ESA-SY-0048
EPS/SYS/SPE/95413
- RD5: NBS: "Data Encryption Standard", Federal Information Processing Standards
Publication 46-2, , Reinforced December 30, 1993



2.3 Data denial objectives

Data distributed via the EPS/ METOP Direct Broadcast Services (LRPT/ HRPT) may be denied to a group of users during a certain period on request of the US Government.

The objectives and general implementation requirements of data denial are described in RD1, ("Procedures and Process For Decision Making and Implementation of Data Denial on US Instruments").

The points relevant to the technical implementation, are summarized below:

- 1- *"U.S. Cabinet-level authority assess whether a crisis or war situation exists, or is developing, which would require selective denial of critical data from U.S. provided instruments on METOP-1 and -2 to an adversary."*

	EUMETSAT POLAR SYSTEM	EUMETSAT 
		Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97

2- Senior NOAA official briefs EUMETSAT Director on the situationand requests EUMETSAT Director to implement data denial:

- to a specific user;
- to a group of users;
- to a geographic region; or
- to all users except the pre-defined list of users (including EUMETSAT and its Member States' national meteorological services) who will always receive data on the understanding that none of these users will redistribute data;
- within a specific time frame (...120 days or more)....”

Note: the final wording will be implemented when agreed between EUMETSAT and **NOAA**.

The encryption system defined in the EPS Encryption system (RD2), approved by the EUMETSAT bodies for the MOP/MSG Programme, and based on the DES-3 encryption algorithm, will be used to implement the data denial requirements.



Consequently, the implementation of data denial will use the same space and ground hardware devices developed for encryption. Data denial aspects will be treated by a dedicated mode of operations using a specific list of privileged users. EUMETSAT has acquired a sound experience in encryption through the METEOSAT Programme and has used European experience developed in industries for military programs to consolidate the specific aspects of data denial.

To allow the understanding of the implementation of data denial scheme, this document provides a detailed description of the EPS encryption system, before addressing the implementation of data denial..

2.4 Structure of the document

This document is structured as follows:

- Chapter 2 gives the overall background of the EPS encryption system, the justification for DES-3 choice, its suitability to the data denial, and a description of its integration in the EPS/METOP Data Handling System.
- Chapter 3 describes the implementation procedures of data denial.
- Chapter 4 summarizes security features associated to the EPS encryption system.

	EUMETSAT POLAR SYSTEM	EUMETSAT 
		Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97

3 ENCRYPTION SYSTEM TECHNICAL DESCRIPTION

3.1 General background

The control of the enforcement of the EUMETSAT data policy for the Polar Orbiting missions is envisaged by means of data encryption facilities on-board the satellite. The HRPT and LRPT channels will have the capability to be encrypted like the MSG HRIT and LRIT data. The DES standard (RD5) is an algorithm in the public domain, which is adequate for data rate in the order of magnitude of the HRIT and HRPT data rate (around 2 and 4 Mbps). The choice of this algorithm contributes to the coherence of the design of the EUMETSAT encryption Center.

The overall EPS encryption technical background could be summarized as follows:



The EPS Encryption System provides the control of the access to the LRPT / HRPT services by registered users; it is composed of the 3 following components:

- the Key Management Center, element of the EUMETSAT Encryption Center, in charge of the management of the all EPS Encryption System, including Keys generation and distribution, monitoring and control.
- the Satellite encryption equipment (part of the METOP satellite Data Handling System)
- the local users decryption units located in the HRPT/ LRPT stations, further described in 2.2.3.

The encryption of HRPT data and the selective access of HRPT / LRPT US instruments data in case of crisis are under the control of the Key Management Center (KMC), which functions will be shared with the MSG Programme within the EUMETSAT Encryption Center. The tasks of the Key Management Center include:

- user station request reception and user registration
- encryption scheduling
- generation of public satellite and user station keys,
- generation (programming) of the secret satellite and user station key media,
- Station Key Unit (SKU) distribution to the registered users
- distribution of satellite via telecommands and station Public Keys (PBK) via public ground networks.
- implementation of data denial for US instruments data as requested by the US Government.

The KMC coordinates its short, medium and long term activities with the EPS /METOP Control Center. These activities can be, for example, the update of keys for certain group of users or the change of keys parameters on board.

	EUMETSAT POLAR SYSTEM	EUMETSAT 
		Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97

The encryption is done on-board the METOP satellite, after acquisition of instruments observational data by the METOP satellite Data Handling System.

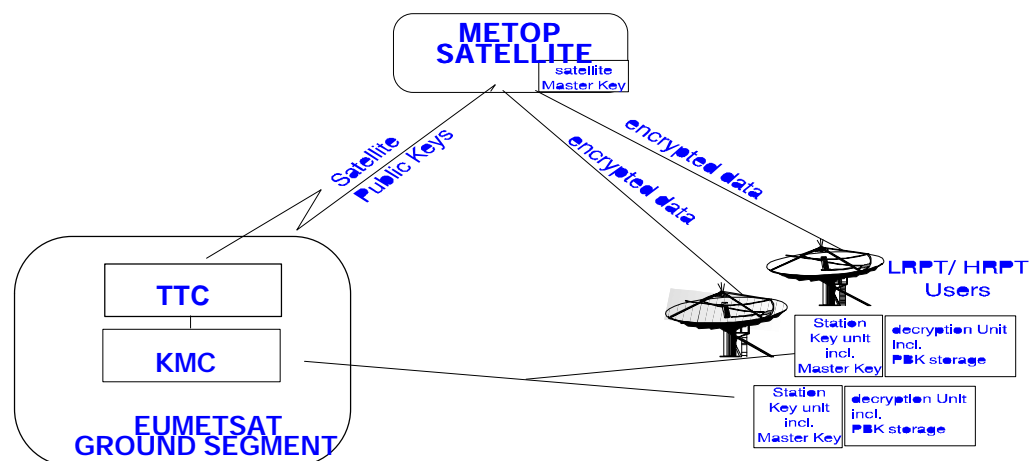




Figure 1: Overall EPS Encryption System

The METOP satellite Data Handling System, performs the following functions:

- Instruments data acquisition under the form of CCSDS packets.
- Data multiplexing into different virtual channels.
- Data formatting into CCSDS Virtual Channel Data Units (VCDU).
- On-board encryption of selected instruments VCDU.
- Reed - Solomon encoding of VCDU.
- Instruments global data storage and transmission via X-band.
- Local data transmission via LRPT / HRPT. The Direct Broadcast services requirements are detailed in RD4.

The actual Encryption Specification follows the Data Encryption Standard (RD05) already used for the encryption of the Meteosat Operational Programme (MOP) data, although MOP data encryption is fully done on -ground: it is based on the following concept:

- The encryption scheme is selective on virtual channels and users stations for both LRPT and HRPT. HRPT and LRPT links are independently encrypted. The contents of the different virtual channels is addressed in 2.3.2.
- Encryption of the data, generation of Message Keys from the uplink of encrypted Public Satellite Keys, is be done in the spacecraft.

	EUMETSAT POLAR SYSTEM	EUMETSAT 
		Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97

- The Message Key controls the encryption process. One Message Key is used for one encrypted Virtual Channel at a time. On board the satellite, the Message Key is generated from a secret Satellite Key and a public (uplinked by TC) Satellite Key. On the ground, the Message Key is reconstructed from a secret Master Station Key and a public Station Key (distributed by ground media).
- The DES-3 implementation of the DES standard has been selected for its adequacy in the security of the encryption algorithm and its strength against hackers. The DES-3 will encipher 64-bits blocks of data successively with 3 different 56-bit keys.

Note: the DES standard is one of the safer codes available in the public domain, and is used commonly for confidential data distribution. It is currently possible to break it by means of brute force: if the 56-bit key is randomly chosen, the only way to break it is by trying the 2^{56} possible keys (70,000,000,000,000,000). Using the triple DES (DES 3) which consist in the encryption of 64 bits of data using 3 different 56-bits keys successively, increases this number to 2^{168} ($5 \cdot 10^{47}$). Hardware and software implementations are available. Dedicated studies have shown that the only possible attack to break DES-3 by crypto-analysis is the related key attack and that this attack can be prevented by **authentication of the Station Public Keys** (this implementation making it impossible to try other Public Key than the one generated by the Key Management Center).



3.2 EPS / METOP Encryption concept

Encryption and decryption are performed within the virtual channel access sublayer of the CCSDS standard. A set of Instruments data (source packets) which are multiplexed into a virtual channel may be encrypted depending on an access criterion predefined by the Encryption Manager.

3.2.1 DES Keys definition

The encryption scheme is selective on virtual channels and on users; it is based on the DES-3 or triple DES implementation of the NBS "Data Encryption Standard". The triple DES implementation selected for EPS corresponds to 3 sequential DES encryption processes (ENC-ENC-ENC) using 3 independent DES keys. DES is a symmetric conventional algorithm, i.e., the same secret key (Message Key) is used for encryption and decryption. The decryption process is symmetrical to the encryption process with inversion of the subkeys orders (DEC-DEC-DEC).

A standardized DES cryptographic key consists of 64 bits, 56 of which are used by the algorithm (forming the active key) and 8 of which are used to detect errors within the key.

	EUMETSAT POLAR SYSTEM	EUMETSAT 
		Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97

A DES3 key consists of a concatenation of three ‘single’ DES keys (Key(1), Key(2) and Key(3)).

DES3 Key		
DES Key(1)	DES Key(2)	DES Key(3)
56 bit key(1) + 8 bit parity K(1,1), K(1,2), K(1,3), ... , K(1,64)	56 bit key(2) + 8 bit parity K(2,1), K(2,2), K(2,3), ... , K(2,64)	56 bit key(3) + 8 bit parity K(3,1), K(3,2), K(3,3), ... , K(3,64)

notation of K(a,b): a = DES Key number, b = DES Key bit number

The encryption system uses four types of keys:

- Master Keys (MSK)
- Message Keys (MGK)
- Public Keys (PBK)
- Pseudo-Noise Keys (PNK)

Master Keys (MSK)

Master Keys are **fixed** secret elements, which are used for:

- Public Keys generation (MGK encryption) at KMC level
- Public Keys (PBK) decryption at ground station level

Message Keys

Message Keys are **static** secret elements, which are updated periodically according to operational issues. An MGK is allocated to a predefined virtual channel for an operational environment (*current or deferred use, data denial*).



Public Keys (PBK)

Public Keys are **static** non-secret elements, which are derived from the MGK by encryption; they are as well updated periodically according to operational issues.

Pseudo-Noise Keys (PNK)

These keys are **dynamic** elements, which are used to generate the PN Pattern sequence; they are generated at each VCDU from the MGK and the expanded seed.

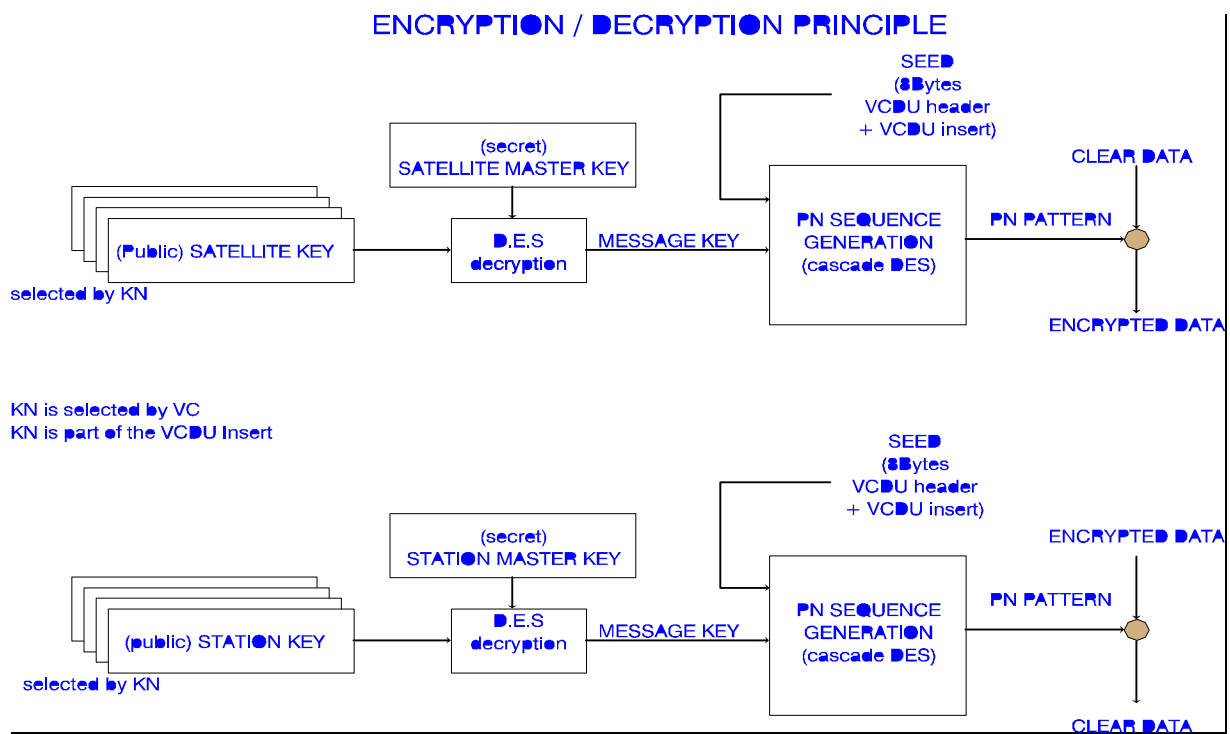
3.2.2

	EUMETSAT POLAR SYSTEM	EUMETSAT 
		Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97

3.2.3 Encryption / decryption principle



The encryption process is controlled by the so-called Message Key (MGK). One Message Key is associated to one Virtual Channel to be encrypted. On-board the satellite the Message Key is retrieved from a Satellite Master Key (MSK) and a Public Satellite Key (PBK) using a triple DES decryption operation. The Public Satellite Keys are selected on board from the Public Satellite Keys table and are addressed by the Key Number (KN). The Key Number table defines whether a virtual channel is encrypted or not and, if encryption is enabled, the related Key Number. A detailed summary of the VCDU contents is given in RD4 and annex 1.

Encryption is performed by multiplying the contents of the VCDU Data Unit Zone with a pseudonoise pattern. Decryption requires a multiplication of the data retrieved from the VCDU data unit zone with the same (reconstructed) pseudonoise pattern. The VCDU insert zone contains both an encryption flag (determining whether this VCDU is encrypted or not) and the Key Number identifying the Message Key.



Message Keys updates

Message Keys are generated randomly by the Key Management Center (KMC) and replaced periodically to ensure sufficient secrecy and control the access. They are then **encrypted by the KMC to generate Satellite or Station Public Keys**; these Public Keys will be transmitted, either to the Satellite via Telecommands, or the Users Stations by various ground media.

	<p style="text-align: center;">EUMETSAT POLAR SYSTEM</p>	<p style="text-align: center;">EUMETSAT</p> 
		<p>Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97</p>

In each User Station, the Message Key is reconstructed from a secret Station Master Key and a Public Station Key (selected using the Key Number).

Every user receives a station Public Key Table containing Public Station Keys records for each of the Message Key that they are allowed to be used (authorized VC) at a given time. The Public Station Keys records are accompanied by the related Key Number, the Station Number, which identifies the addressed user; to each PBK is appended an authentication trailer (MAC field) used to authenticate the station PBK, and a CRC trailer to check the integrity of the PBK record (*the authentication field, ensures that the station PBK and the Station Key Unit (SKU) will not be used for any other purpose than the reception of the authorized Virtual Channels by the station*). The addressed user only is capable of decrypting the Public Station Keys properly, using its own, permanent, and (secret) Station Master Key so that the secrecy is not impaired by the distribution of either the Satellite or the Station Keys.

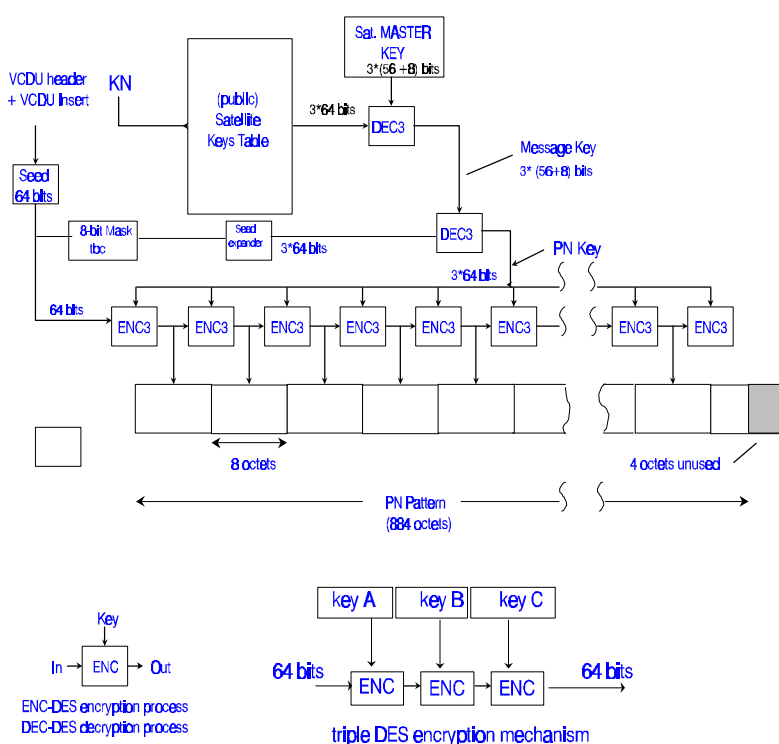




Figure 2: On board encryption architecture

The figure above summarizes the on-board encryption concept.

	EUMETSAT POLAR SYSTEM	EUMETSAT 
		Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97

The encryption procedure follows the sequence below:

- key selection and generation of insert data
- message key generation
- pseudonoise pattern generation
- data transformation

The decision on whether the data is to be encrypted and the selection of key pattern shall be performed on basis of the VCDU-ID.

Key Selection and Insert Generation

For this procedure the VCID (6 bits) is used as input. As output, the key selection provides 16 bit insert data containing the encryption control information.

The Key Number Table contains, for each virtual channel, a 16 bits record with the appropriate encryption control information: encryption flag (1 octet) and Message Key Number (1 octet). When **encryption is enabled, the encryption flag shall be set to FF**, otherwise it shall be set to 00.

The appropriate record of the Key Number Table is selected with help of the virtual channel number contained in the VCDU-ID. The contents of the selected record is copied into the insert zone of the VCDU.

Message Key Generation



The Message Key is a triple DES Key (corresponding to 3 *(56+8) bits) generated randomly by the Key Management Center (KMC) and updated regularly. It is re-generated on-board by decrypting the associated Public Satellite Key corresponding to the selected Key Number through a DES-3 decryption process, using the Satellite Master Key as the key pattern.

64 Public Satellite Keys, allowing to generate up to 64 different Message Keys, can be stored in a Public Key Table indexed by the Key Number for **each** LRPT and HRPT channel. Separate Public Keys Tables shall be provided for LRPT and HRPT channels.

Pseudo Noise data generation

Pseudonoise data is generated by repetitively routing data through the DES-3 encryption process. With each cycle 64 bits of PN data are generated.

As initial input (seed), the concatenated contents of VCDU header and insert zone is used. All DES processes are performed using a Pseudo-Noise key pattern generated by routing and expanding the seed through a DES decryption process, using the Message Key as key pattern. A Pseudo-Noise

	EUMETSAT POLAR SYSTEM	EUMETSAT 
		Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97

Key will be composed of 3 *64-bits keys which will successively activate the DES-3 encryption algorithm.

3.2.4 Stations decryption concept

The decryption procedures shall be embedded in the task "VCDU acquisition".

After applying Reed-Solomon FEC to the received VCDU, and the check symbols are stripped off, resulting in a VCDU, the content of the Insert zone will tell if the VCDU has been encrypted.

The decryption activities are similar functions to those implemented for encryption:

1. Insert zone analysis (to check if the VCDU is encrypted and extract the related KN and PBK)
2. generation of the appropriate message key
3. generation of the pseudonoise pattern
4. VCDU data unit zone decryption

In parallel, a PBK authentication function will verify the PBK correctness of the MAC field for the ground station.



Up to **64 Public Station Keys** reports can be stored within the Key Unit in a station Public Key Table indexed by the Key Number. The Public Station Keys reports contain: a 192 bits long- PBK, a field containing the Message Authentication code (MAC of 64 bits) for PBK authentication purpose and a Cyclic Redundancy Checksum (CRC, 1 byte).

The PBK CRC is checked at the PBK record set reception.

The MAC is checked at PBK update and during each PNK generation.

This concept will be implemented on ground in 2 elements:

- The Station Key Unit, containing the Secret Station Master Key (MSK), generating the MGK/ PNK, implementing the PBK authentication, and distributed by EUMETSAT.
- The decryption unit, containing the PBK database, performing the PNP generation and VCDU decryption, procured by the user.

	EUMETSAT POLAR SYSTEM	<div style="display: flex; justify-content: space-between; align-items: center;"> <div style="font-weight: bold; font-size: 1.2em;">EUMETSAT</div>  </div> <div style="margin-top: 10px;"> Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97 </div>
---	--------------------------------------	---

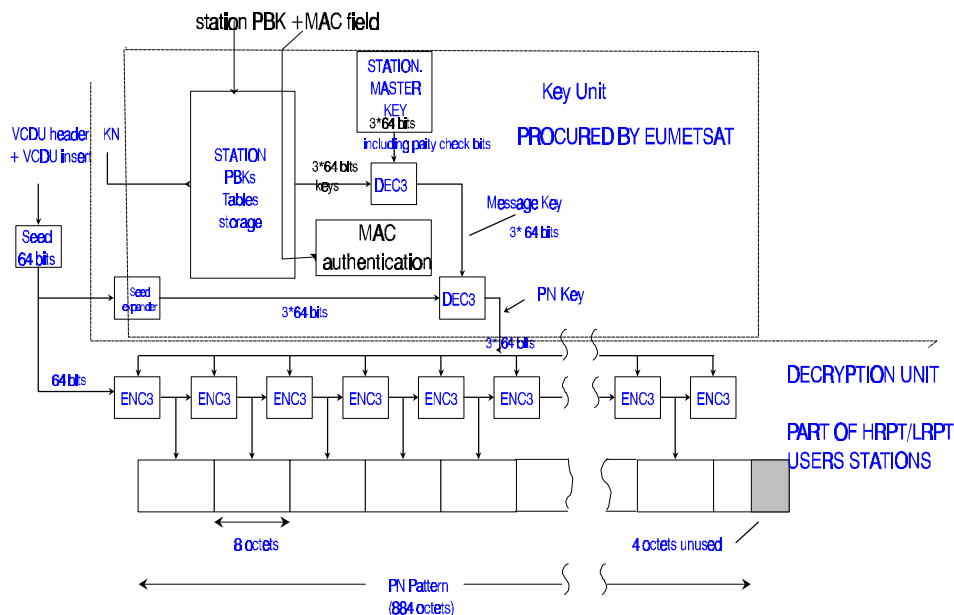


Figure 2: ground station decryption unit design

3.3 Keys Management concept

The EPS Encryption System Management function covers some of the following activities:



- HRPT / LRPT users registration and data access management
- encryption scheduling (decision to update the PBK/ MGK)
- generation of users Master Keys / Public Keys

3.3.1 Users station registration and data access management

Each user station, which wants to receive LRPT or HRPT data, will have to be registered and authorized by the Key Management Center (KMC).

For each agreed user, the KMC will do the following tasks:

- allocate a User Id .
- generate a user LRPT or HRPT MSK, and burn it into the Station Key Unit to be sent to the user.
- store the user data with the User Id in a EPS encryption database containing:
 - the list of enabled Virtual Channels (and related MGK) for the user
 - starting and ending date for each service

	<p style="text-align: center;">EUMETSAT POLAR SYSTEM</p>	<p style="text-align: center;"><i>EUMETSAT</i> </p>
		<p>Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97</p>

- access to METOP-2 specific VC (during commissioning)
- type of user: privileged or to be denied.
- update this information when required: new request from the user, user service duration check, modification of the users access rights for data denial, user account
- during the time the user is registered, the KMC will generate the user authenticated PBKs corresponding to the user profile, and transmit them to the user via requested media.

All registered user information concerning data encryption / denial, will be structured in the EPS Encryption database by the KMC.

A table will address the decryption unit provided to the user and will contain the following parameters:

- | | |
|-------------------------|---|
| • Id | User id |
| • Channel | HRPT , / LRPT |
| • Address: | |
| • List of accessible VC | during nominal access mode |
| • Beginning of service | |
| • End of service | |
| • Acknowledgement | PBK acknowledged after reception |
| • Privilege | the user is part of the authorized list for the access to denied data |
| • Master Key | programmed in the key unit |
| • communication | for PBK distribution |

The user MSK will remain secret to the KMC operator.

A user table can be modified: a user can be deleted or added; its parameters can be edited and changed.

3.3.2 On board encryption configuration

The KMC controls the on-board encryption configuration via the management of the KN table and the satellite PBK table part of the EPS Encryption database.

The table below shows the allocation of the different instrument data to HRPT and LRPT channels and to predefined Virtual Channels.



	<p style="text-align: center;">EUMETSAT POLAR SYSTEM</p>	<p>EUMETSAT </p> <p>Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97</p>

Table1: instrument data transmission via HRPT or LRPT channels

	HRPT / LRPT Transmission	Virtual Channel Identifier
Spacecraft Housekeeping	HRPT / LRPT	34
MHS	HRPT / LRPT	12
AMSU A1/2, SEM, HIRS	HRPT / LRPT	3
AVHRR High rate	HRPT	9
AVHRR Low rate	LRPT	5
DCS	HRPT	27
IASI	HRPT	10
ASCAT	HRPT	15
GOME	HRPT	24
GRAS positioning data	HRPT / LRPT	34
GRAS sounding data	HRPT	29
Adm. messages	HRPT / LRPT	34
fill VC	HRPT / LRPT	63

VC 34 and 63 are never encrypted.

Table 1 shows that:



- Up to 3 VC are to be encrypted (for data denial) on LRPT: 3, 5 12.
- A maximum of 8 VC are to be encrypted on HRPT: 3, 9, 10, 12, 15, 24, 27, 29.

The **KN table** contains the status (Clear or Encrypted) of each virtual channel, and the Key Number associated to each encrypted VC. 64 Key Numbers are allowed for each LRPT and HRPT channels.

VCID	3	5	9	10	12	15	24	27	29
HRPT configuration	C/E	N/A	C/E	C/E	C/E	C/E	C/E	C/E	C/E
HRPT Key Number if conf.= E*	0		1	2	3	4	5	6	7
LRPT configuration	C/E	C/E	N/A	N/A	C/E	N/A	N/A	N/A	N/A
LRPT Key Number if conf.= E*	0	1			2				

C = Clear; E = Encrypted. *: KN are given for example

The PBK table contains the set of PBK mapped to the Key Numbers.

	<p style="text-align: center;">EUMETSAT POLAR SYSTEM</p>	<p style="text-align: center;">EUMETSAT </p>
		<p>Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97</p>

For each channel, a maximum of 8 Key Numbers (up to 8 encrypted VC for HRPT) need to be selected; these 8 Key Numbers will constitute a Key Numbers Set (KNS), which will address a PBK subtable of 8 PBK; up to 8 PBK subtables can be created.

The KN set / PBK subtable correlation for each LRPT or HRPT channel looks like the following table:

Key Number Set	Key Number (index)	PBK table partition
#1	0 to 7	subtable 1
#2	8 to 15	subtable 2
#..
#7	48 to 55	subtable 7
#8	56 to 63	subtable 8

The possibility to have 8 PBK subtables will allow to allocate:

- a subset for current use
- the next PBK subset for the next period
- a subset for data denial (restricted access)
- a subset for data denial (restricted access) for the next period
- four subsets are available for METOP 2 or for an additional list of privileged users (if necessary).

3.3.3 Encryption scheduling; MGK generation

For each LRPT and HRPT channels, for each satellite (METOP-1 and -2), at each key change period, the KMC will generate as a minimum:



- one MGK subset to be used in normal access mode (NDM)
- one MGK subset to be used in restricted access mode (RDM)

The MGK will be computed using a software PN generator.

8 MGK subsets can be generated; this let room to implement if necessary, different lists of privileged users.

The KMC will, then, generate the corresponding satellite PBK subset by 3 x DES-3 encryption of each MGK of the MGK subset by the satellite MSK. Each PBK subset will be associated with a KNS.

The satellite PBK and KN tables will be updated by telecommands, with a time of execution. A corresponding control file will be generated to keep track of all modifications of the tables.

	EUMETSAT POLAR SYSTEM	EUMETSAT 
		Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97

4 DATA DENIAL: OPERATIONAL PROCEDURES

As explained in the above section 2.3, the HRPT and LRPT data can be accessed in two modes:

- Normal Data access Mode (NDM)
- Restricted Data access Mode (RDM) for *quasi- immediate* Data denial.

Normal Data access Mode is the routine mode for data access; when a user registers, he will receive a SKU; then, as described in 2.3, the KMC will update regularly a subset of NDM Key numbers, Message Keys and Public Keys which will be distributed to the satellite and the registered users.

When the request of Data Denial is given, the satellite will go *quasi- immediately* to RDM: a RDM telecommand will switch the encryption Key Number subtable in use to the RDM specific Key Number subtable (see 2.3.2); the RDM specific set of MGKs will be used by the satellite encryption units and decryption units; these MGK will be computed from the satellite RDM PBK subtable already stored on-board, and from the users RDM PBKs subtable. Only those pre-defined privileged users will have received the RDM PBK subset. Some additional procedures will have to be introduced to modify the list of users to be denied as seen below in 3.1.



4.1 Director's list

Once a User has requested an HRPT or LRPT service, EUMETSAT verifies if he can be registered, and if he is entitled to restricted access for data denial; this is done according to a pre-established scheme agreed with the US Government (or after consultation with the US Government on a regular basis). He will then be given a Decryption Unit and will receive periodically a set of PBK corresponding to his request and entitlement.

The Agreement (item 4) states that "Senior NOAA official consults with EUMETSAT Director and conveys to him the determination of the U.S. Cabinet level authority. Senior NOAA official requests EUMETSAT Director to implement data denial:

1. to a specific user;
2. to a group of users;
3. to a geographic region; or
4. to all users except the pre-defined list of users (including EUMETSAT and its Member States' national meteorological services) who will always receive data on the understanding that none of these users will redistribute data
5. within a specific time frame."

This requirement will be implemented by denying data access at user station level, i.e., the user will be associated to its Station Key Unit.

	EUMETSAT POLAR SYSTEM	EUMETSAT 
		Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97

The **Director's list** will be created according to policy criteria set in bullet 4 above. It will serve as the core Restricted Access list to which EUMETSAT will start from when data denial is requested for. These "privileged users" will be distributed an additional subset of PBK to be stored in their PBK database. This core list could be updated if the US Government and / or EUMETSAT agree to do so.



4.2 Sequence of actions

Before the decision is taken to implement data denial, 2 types of actions can be considered:

1. Establishment of a Core List of Users and updates when necessary (every tbd months as part of a routine operation of the EPS System).
 - This operation requires inputs and approval from the EUMETSAT Director.
 - Its implementation lasts few days depending on the EPS System scheduling activities.
2. Following the precursory signals of a Crisis, a Crisis Group will be settled to check the last revision of the list and update it if necessary.
 - When? Few weeks before the data denial decision.
 - How long? Between 2 days and a week depending on the number of Users to be denied.

When the Decision to implement data denial is taken, the following sequence of events will be implemented:

1. set the encryption to Minimum Restricted Access list; this operation will be executed by sending the command "Switch to RDM KNS subset..." to the METOP satellite;
 - Who? The S/C Control Center
 - When? As soon as the decision is received to the METOP Control Center
 - How long? Within few passes (few hours)
2. inform the users that the Restricted Access Mode is entered (via an admin. Message or e-mail);
 - Who? The KMC and Control Center
 - When? It starts as soon as the command has been transmitted
 - How long? To be finalized at a later stage.
3. update the MGKs for the following "normal" period;
 - Who? The KMC.
 - When? ASAP after 2 is achieved.
 - How long? Less than a working day.

	<p style="text-align: center;">EUMETSAT POLAR SYSTEM</p>	<p>EUMETSAT </p>
		<p>Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97</p>

4. compute new PBKs for the satellite and the users stations;
 - Who? The KMC.
 - When? ASAP after 2 is achieved.
 - How long? Less than a working day.
5. load the new satellite PBK via Telecommand “update PBK table:
 - Who? The Control Center
 - When? Anytime during METOP routine operations..
 - How long? During a pass, depending on the Short Term Plan availability;
6. distribute new PBK to the **allowed users** with the date of use;
 - Who? The KMC
 - When? ASAP after 4 is achieved; one day to one week after RDM, depending on EPS System tasks priorities, and of number of “privileged users”.
 - How long? Less than a week.
7. send FMU command “switch to KN Table subset 8 to 15”.
 - When? After 5 is achieved; 2 days to a week after RDM.
 - How long? Within few passes.



It should be noted that:

- The data denial can be rapidly implemented
- The duration of exclusion can be modified if required.
- The update of users PBKs is the critical element of the chain of operations due to the number of users, even if some of these operations can be highly automated: the KMC will have to generate and send new PBKs to around **15000 LRPT and HRPT users**, as well as to verify (via acknowledgement of the users) that all allowed users will have received the new set of PBKs.

4.3 Instrument’s list

Data denial can address one or several instruments which selection will be made in advance during nominal operations. Only the PBK/KN corresponding to the instruments to be denied will be modified. This list will be agreed between EUMETSAT and NOAA.

4.4

	EUMETSAT POLAR SYSTEM	EUMETSAT 
		Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97

4.5 Additional Security features

4.5.1 Master Keys

The satellite and stations Master Keys are burnt into PROM and cannot be accessed by hackers. The information on these keys will remain secret.

The Satellite and System tests will be done using a satellite test MSK, which will be replaced before launch.

The Satellite Master Key transfer will be protected during replacement before launch. No access to the information will be possible by non mandated personal.

4.5.2 Authentication of Users Stations Public Keys

Users Stations Public Keys will be authenticated in order to guaranty that the Decryption units sent to the registered user will not be used for other purposes than the decryption of the HRPT/ LRPT services, and that the PBK distributed to the particular user via the public network cannot be used without the specific Decryption unit.

The 64 bits long Message Authentication Code (MAC) will be computed at the KMC, based on DES-3; it will not be possible to derive the secret keys from the PBK and MAC.



4.5.3 Key Management Center protection

The access to the KMC will only be given to accredited personal.

4.5.4 Users Stations Master and Public Keys distribution

The distribution of Key Units containing the Station Master Keys will be done by special postage.

Public Keys can be distributed by non-secured means (fax, e-mail,...), provided that they are authenticated.

	EUMETSAT POLAR SYSTEM	EUMETSAT 
		Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97

Annex 1 : Network layer: VCDU description

The Data Link Layer is organized into two sublayers: a Virtual Channel Link Control sublayer (VCLC) and a Virtual Channel Access sublayer (VCA). The VCLC sublayer receives CCSDS packets from the Network layer, while the VCA sublayer forwards the physical channel access protocol data unit (PCA_PDU) to the physical layer.

The virtual channel procedures are functions required to generate virtual channel data units (VCDUs) from VCA_SDUs and vice versa. One of the channel access procedures is to handle Reed-Solomon check symbols. A VCDU with attached check symbols is called coded virtual channel data unit (CVCDU). The PCA_PDU consists of a succession of CVCDU prefixed by a Synchronization Marker.



The structure of one CVCDU is shown in the following figure.

VCDU Primary Header (6 octets)					VCDU insert zone 2 octets	VCDU Data Unit Zone		CVCDU Check symbols 128 octets	
Version n° "01"	VCDU Id		VCDU counter 3 octets	Signaling Field 1 octet		M_PDU header 2 octets	M_PDU packet zone 882 octets		
	S/C id 8 bits	Type 6 bits		Replay flag "0"		spare "0000000"	M-PDU header spare		M_PDU first header pointer

1 VCDU primary header

The VCDU primary header consists of the following elements:

version number	set to "0 1" specifying version-2 CCSDS structure
VCDU-ID	virtual channel data unit identifier as specified in Chapter 4, consisting of spacecraft identifier and virtual channel identifier.
VCDU counter	sequential count (modulo 16777216) of VCDUs on each virtual channel
signaling field	set to 0 specifying real-time VCDUs

	EUMETSAT POLAR SYSTEM	EUMETSAT 
		Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97

2 VCDU Insert Zone

The insert zone is used for encryption control.

The structure of the IN_SDU used with LRPT or HRPT is as follows:



The insert service data unit (IN_SDU) is used for data encryption: this field is composed of:

- Encryption flag (1 octet): set to 00HEX when encryption is off; set to FFHEX when encryption is on.
- Key number (1 octet): this octet indicates which message key is used to encrypt the VC. It is set to 00HEX when encryption is off.

3 VCDU Data Unit Zone



The CVCDU data unit zone contains the multiplexing protocol data unit; this field consists of:

- M_PDU Header Spare bits (5 bits) : all set to "0"
- M_PDU Header First Pointer (11 bits): it contains a binary count P, which, when incremented by one, points directly to the number of the octet that contains the first octet of the first CCSDS packet header. If the VCDU data zone does not contain any packet header at all, the bits shall be set to "1".
- M_PDU Packet Zone (882 octets): it contains part, parts or complete CCSDS packets.

	EUMETSAT POLAR SYSTEM	EUMETSAT 
		Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97

LIST OF ACRONYMS

AMSU-A	Advanced Microwave Sounding Unit A
AMSU-B	Advanced Microwave Sounding Unit-B
ASCAT	Advanced Scatterometer
AVHRR	Advanced Very High Resolution Radiometer
ESA	European Space Agency
EUMETSAT	European Organisation for the Exploitation of Meteorological Satellites
GOME	Global Ozone Monitoring Experiment
GRAS	GNSS Receiver for Atmospheric Sounding
G/S	Ground Segment
HIRS	High resolution Infrared Radiation Sounder
HRIT	High Resolution Image Transmission
HRPT	High Resolution Picture Transmission
KN	Key Number
KNAT	Key Number Access Table
IASI	Infrared Atmospheric Sounding Interferometer
IR	Infra-Red
LRIT	Low Resolution Image Transmission
LRPT	Low Resolution Picture Transmission
MAC	Message Authentication Code
METOP	Meteorological Operational satellite
MGK	Message Key
MHS	Microwave Humidity Sounder
MSG	Meteosat Second Generation
MSK	Master Key
NOAA	National Oceanic and Atmospheric Administration
NDM	Normal Data access Mode
PBK	Public Key
PNK	Pseudo Noise Key
RDM	Restricted Data Access Mode

	<p>EUMETSAT POLAR SYSTEM</p>	<p>EUMETSAT </p>
		<p>Doc No : EPS/SYS/TEN/96895 Issue : 1a Date : 16/06/ 97</p>

RD	Reference Document
S&R	Search and Rescue
SEM	Space Environment Monitor
SRD	System Requirements Document
VCDU	(CCSDS) Virtual Channel Data Units
TBC	To Be Confirmed
TBD	To Be Determined
TIROS	Television Infra-Red Observing Satellite